[Call for Participation]

Title: **From Practice to Theory: Cryptology and Cyber Resilience**

Dates: 19 - 26 July 2015 (Sunday - Sunday)

Format: summer school - One intensive week of theory, practice and discussions: 4-hour lectures and tutorials by international experts extended with practical workshops, labs and seminars, simulations, round-table discussions and working groups on hot topics

Place: "National Institute of Education", Oriahovitza, Bulgaria

Organizers: Balkanski-Panitza Institute for Advanced Studies (BPIAS): www.bpias.org
European Software Institute Center Eastern Europe (ESI CEE): www.esicenter.bg
Minu Balkanski Foundation: www.balkanski-foundation.org
[and IT industry, academic partners, law-enforcement and defense authorities]

SUMMER SCHOOL PROFILE

To prepare the researchers and IT practitioners for the digital security and resilience of our e-business and e-life TOMORROW, we must foresee and develop on what will be AFTER TOMORROW.

The focus of this Fourth summer school is to ***Bridge the Practice to Theory*** by gathering world class leaders in the field with young researchers, IT security practitioners, e-business innovators, business resilience managers and cyber-defense professionals. The School will build on the CryptoBG*2012 – CryptoBG*2014 and the earlier International Symposiums on Recent Developments in Cryptography and Information Security. The topics answer the e-competences demand for modern industry and society, aligned with the Europe 2020 Digital Agenda, the NATO Smart Defense initiative and Multi National capacity development (addressing 2035+).

The Summer School is a milestone of a longer-term joint program of the organizers (BPIAS, ESI CEE, Minu Balkanski Foundation, and international partners), composed by trainings on IT and information security (form schools to universities), series of lectures and visiting speakers at, awareness campaign for the civil digital society, and forming an operational Cyber-Defense cluster.

The latest trends and state-of-the-art open problems are linked to practical aspects and case studies on use or miss-use of the information, our digital identity and trust. We want to foster forming the Bulgarian research and scientific community, serving the IT industry, all IT-enabled services (like banking, e-Health, e-Administration, industries), and the Knowledge Society in Bulgaria and the entire region.

It starts with encoding messages and providing confidential sender-receiver channel, the basis of ***Cryptography***. Numerous mathematical methods, such as number theory, combinatorics, coding theory, complexity theory and algorithms, are applied for secure transmission of messages. Fast-growing technologies serve both the healthy and the dark side. The challenge is to construct high-complexity encodings that would still take millions of years for decoding with the most powerful supercomputer and the most efficient known attacks. ***Cryptography*** is practically everywhere, in all software or hardware system – internet, emailing, mobile devices, access control and password authentication, digital signatures, network and systems security.

Cryptography is the basis, but not a guarantee for the Cyber Security and ***Cyber Defense*** – the complex area which controls the risks related to the use of various computer systems and creates computer platforms, languages and applications according to established security rules and compliances. Here we combine technologies with methodologies, organization and awareness for higher internet security, systems and mobile security, content protection, digital rights management, and more general – resilient and sustainable operations at all levels and areas.

MAIN TOPICS AND PROGRAM

Topics of the year – the specific focus areas for 2015 edition will be:

- **Crypto for cloud** – Searchable encryption and Homomorphic encryption (with practical simulations and demo-kit)
- Crypto and security for **smart devices** – Internet of Things, the emerging standard of "industrial Internet", theory and practice (semi-autonomous, robots) – specific aspect: Side channel attacks

Theory

- elliptic curve cryptography (ECC), symmetric key, lattice-based cryptography
- efficient arithmetic and integer factorization
- functional encryption – identity-based encryption (IBE) and attribute-based encryption (ABE
- curve-based cryptography – theoretical and practical aspects
- pairing-based cryptography
- blind signatures and e-voting schemes
- secure communications

Practice

- personal secure devices, mobile security
- secure architectures, "security by design" aspects
- biometrics for security, multi-factor security (incl. "intuitive" methods)
- e-Voting – practical realization
- security in the cloud – searchable encryption lab
- side-channel resistance – practical labs and simulation

And your favorite *CTF*BG round (Capture The Flag)* by CyResLab (of ESI CEE) RED <>BLUE teams in 3 sessions:

- CTF "warm up" & challenges explained
- active security – MITM demos, PKI & SSL, Secure Coding digest
- CTF*BG Ultimate

The program will include also several ***discussions*** on hot topics identified by leading companies and partners supporting CryptoBG*2015, organizers and participants themselves.
[The participants will also communicate their results and research topics]

[Preliminary] LIST OF LECTURERS

Dr. Nicolas Gama, Universite de Versailles, France)
Dr. Valerie Gauthier, University of Rosario, Bogota, Columbia (TBC)
Prof. Dimitar Jetchev, EPFL, Switzerland
Dr. Elena Andreeva, KU Leuven, Belgium
Dr. Iosif Androulidakis, Greece
Dr. Mariya Georgieva, Gemalto, France
Dr. Elizabeth Quaglia, Huawei Technologies, France
Prof. Krassimir Manev (TBC)

Workshop with simulations prepared by the CyLab of ESI Center.

Materials: The *CryptoBG*Summer School - Lecture Notes* will be provided to participants for download during and after the summer school (special publication series is under consideration).

WHO SHOULD ATTEND

The Summer School is tailored for researchers, students and professionals involved and interested in these special theoretical and practical areas. Both users and developers of applications will benefit from the program. Industry representatives will discover new opportunities for development and bridging with theory. Authorities using or supporting secure communications and information exchange are welcomed. Cyber-defense professionals and officers will gain both know-how and foresight to meet the "unknown".

LOCATION

The Summer School will take place in the conference center of the National Institute of Education in Oriahovitza, a small village near Stara Zagora. The center is equipped with conference rooms, lecture rooms and computer facilities. Located at the foot of the beautiful Sredna Gora Mountain and famous for its wineries, the village is nowadays hosting various international cultural and scientific events organized by Minu Balkanski Foundation.
Map: http://goo.gl/maps/kBc40

ORGANIZING COMMITTEE

Prof. Minko Balkanski, IHE, France minko.balkanski@balkanski-foundation.org
Dr. George Sharkov, ESI CEE, Bulgaria gesha@esicenter.bg
Prof. Dimitar Jetchev, EPFL, Switzerland dimitar.jetchev@epfl.ch
Mariya Georgieva, Université de Caen, France maria.georgievabs@gmail.com

Administration: Violeta (Via) Kyurdyan, ESI CEE via@esicenter.bg

INVITATION TO PARTICIPATE

You are kindly invited to **participate** or delegate a person from your organization.

Participation fee: *900 BGN/450 EUR/500 USD* (*incl. accommodation, meals, logistics; no transport)*
Please express your interest before ***15 May 2015*** *and return the* ***Registration form before 30 May 2015****!* ***The Registration Form is at www.cryptobg.org !!!***

For Bulgarian students: Limited number of scholarships available, please apply with motivation email (free text), Registration form and a short CV.

For Sponsors: Your support is highly appreciated – as co-funding, student scholarships, or in-kind ***- please contact us for your sponsor package!***

Please address questions and confirm your interest to:

Dr. George Sharkov: gesha@esicenter.bg
Prof. Dimitar Jetchev: dimitar.jetchev@epfl.ch
Organizing Committee info@cryptoBG.org (phone: +359 2 489 9740)

Updated info, and materials from previous CryptoBG*** and downloads: www.cryptobg.org